

they would certainly be found out. If allegations were false, the verdict would be made clear to all.

Senator FRANK LAUTENBERG, like me, is living proof that the American dream can come true. His hard work, determination, and ingenuity brought him from humble beginnings to build with two partners the Automatic Data Processing (ADP) Company, which became the world's largest computing services company.

I was pleased to work with Senator LAUTENBERG on legislation to prohibit smoking on public transportation. He has been a tireless worker in the war to prevent teenage smoking.

To my Democratic colleagues, Senators LAUTENBERG, MOYNIHAN, BRYAN and KERREY: We have battled through many issues, each of us committed to doing what we believed was best for America and for our respective states. There has never been a dull moment. It has been a privilege to work with you.

Last but not least, I have to bid farewell to my fellow Republican and Finance Committee member, Senator CONNIE MACK. His friendship, leadership, and dedication to furthering the causes of fiscal responsibility, governmental accountability, and medical research will be greatly missed.

Senator MACK has successfully fought for Florida's concerns and kept his campaign promise of "less taxing, less spending, less government and more freedom," which resulted in 70 percent of the vote in 1994, more than any other Republican Senatorial candidate in the Nation.

The Roman politician Cicero states, "It is the character of a brave and resolute man not to be ruffled by adversity and not to desert his post."

I believe Senator MACK has been this exemplary leader; and, instead of faltering like most men, Senator MACK had the ability to rise above not one, but three, personal battles with cancer—his wife's, his daughter's and his own. Senator MACK lost his mother, father and younger brother to cancer. This history makes the Mack's the poster family for early detection, a role they have indefatigably played.

Drawing from this experience, Senator MACK has fought to double the funding for National Institute of Health (NIH) in order to step up the search for a cure for cancer as well as other diseases that plague our families and society today. This is a goal I will continue to support not as a legacy for CONNIE MACK, but inspired by him and his family.

It has been a pleasure and an honor to serve with these men, and I want to take this opportunity to bid farewell and best wishes to our colleagues as they begin what I hope will be a very rewarding retirement.

INFORMATION SYSTEMS SECURITY

Mr. HOLLINGS. Mr. President, the General Accounting Office recently concluded that formal software man-

agement policies at eight of the sixteen U.S. Federal agencies they investigated were found to be inadequate and that controls over access to software codes were weak. I am convinced that the information systems used by the Department of Defense are critical components of the warfighting capability of the United States. Off-the-shelf and customized software is critical to the functioning of these systems. I rise today to express my concern that the security and integrity of critical government systems could be at great risk if their operational software has been procured or developed outside the United States or without proper oversight and control. I have read, with growing concern, a number of news articles that suggest that foreign software acquisitions can have potentially catastrophic consequences on both classified and unclassified national information management systems used by Federal agencies for sensitive applications.

I would like to cite just few examples to illustrate my point. An article in the February 16, 2000, Washington Post discussed the State Department's purchase of an unclassified, but sensitive, business operations system with software code developed by former citizens of the Soviet Union. According to the article, State withdrew the system from their embassies worldwide because they were concerned that hidden code might have been added during development and fielding. The final paragraph of the article states: "The lesson of State's fiasco is simple—but so important it should be hard-wired: As people and organizations grow more dependent on computers, they become more vulnerable. It's easy to forget that every line of code can be a potential spy or saboteur."

On March 2, 2000, the New York Times reported that Japanese software suppliers associated with the terrorist sect responsible for the Tokyo subway nerve gas attack had sold software programs to several Japanese government agencies, to include their Defense Ministry. According to the article, the agencies and companies that ordered the software were unaware that the sect was involved because the principal suppliers had sub-contracted the work to others. As recently as June 19, 2000, the Defense News reported that two German defense industry employees were convicted of selling missile secrets to Russia. A software provider could have easily employed these "spies." Unfortunately, this is not a new phenomenon. On October 24, 1999, as we prepared for the Y2K transition, the Los Angeles Times ran an article citing concerns by security experts that the use of foreign contractors for Y2K solutions could have placed critical systems at risk. The article reports that, in the words of one government security expert, "The use of untested foreign sources for Y2K remediation has created a unique opportunity for foreign countries or companies to

access and disrupt sensitive national security and proprietary information systems." The GAO further maintained that background screening policies for personnel involved in Y2K remediation were lacking or inadequate despite at least 85 Federal contracts being completed using foreign nationals.

The Department of Defense routinely purchases software developed by foreign companies. The Department is often unaware of that fact. For many of its unclassified, but critically important, business operating systems, government agencies contract with a systems integrator. The integrator then selects the software system to be installed as part of the operating system. The Agencies are often not aware that the software was developed in a foreign country, by foreign developers, and perhaps, even in a foreign language. I believe that, at a minimum, the provision of software produced by a U.S. company (or at least software controlled by a U.S. company) should be a consideration in the acquisition process. Encouraging the Defense Department (and other Government agencies) to at least consider the origin and ownership of source codes will not eliminate vulnerability, but it is a step in the right direction. Additionally, it reinforces software development as a key component of our defense industrial base. For that reason, I urge the Administration to put in place protocols in the selection process that consider the origin of all source codes used in the development of information systems acquired or developed. This should include those acquisitions arranged via sub-contracts by prime contractors or system integrators.

SUPPORT FOR CHINA COMMISSION INCREASED FUNDING

Mr. BAUCUS. Mr. President, I rise today to speak to the Commerce, State and Justice Appropriations Conference report's recommendation which provides \$500,000 for the congressional-executive commission on China. This noteworthy commission was established in Title III of the China/PNTR bill, which the Senate passed with a strong majority and the President signed into law just two weeks ago.

It is my understanding that the Commission would normally require a funding level of at least \$1.3 million. However, this year the conferees allocated a lesser amount based on the fact that the Commission will operate for less than a full year in FY2001.

Without a doubt, we should fully support the Commission at its requested level of \$1.3 million in FY2002 and subsequent years once members have been appointed, staff hired and the operation is fully functional for an entire fiscal year. While the initial request of \$500,000 is sufficient for the start-up operation of the Commission, it falls far short of the amount required by its enabling legislation and our congressional intent.